531, 843

(12) INTERNATIONAL A ICATION PUBLISHED UNDER THE PATENT CO ERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 May 2004 (21.05.2004)

PCT

(10) International Publication Number
WO 2004/042602 A1

(51) International Patent Classification7: G06F 17/10

(21) International Application Number: PCT/SG2002/000245

(22) International Filing Date: 21 October 2002 (21.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (*for all designated States except US*): STMICROELECTRONICS ASIA PACIFIC PTE LTD. [SG/SG]; 28 Ang Mo Kio Industrial Park 2, Singapore 569508 (SG).

(72) Inventors; and
(75) Inventors/Applicants (*for US only*): PLESSIER, Bernard [FR/SG]; 25 Leonie Hill Road, #06-05 Grangeford, Singapore 239196 (SG). MING, Kiat. Yap [MY/SG]; Blk 248, Jurong East Street 24, #11-62, Singapore 600248 (SG).

(74) Agent: DONALDSON & BURKINSHAW; P.O. Box 3667, Singapore 905667 (SG).

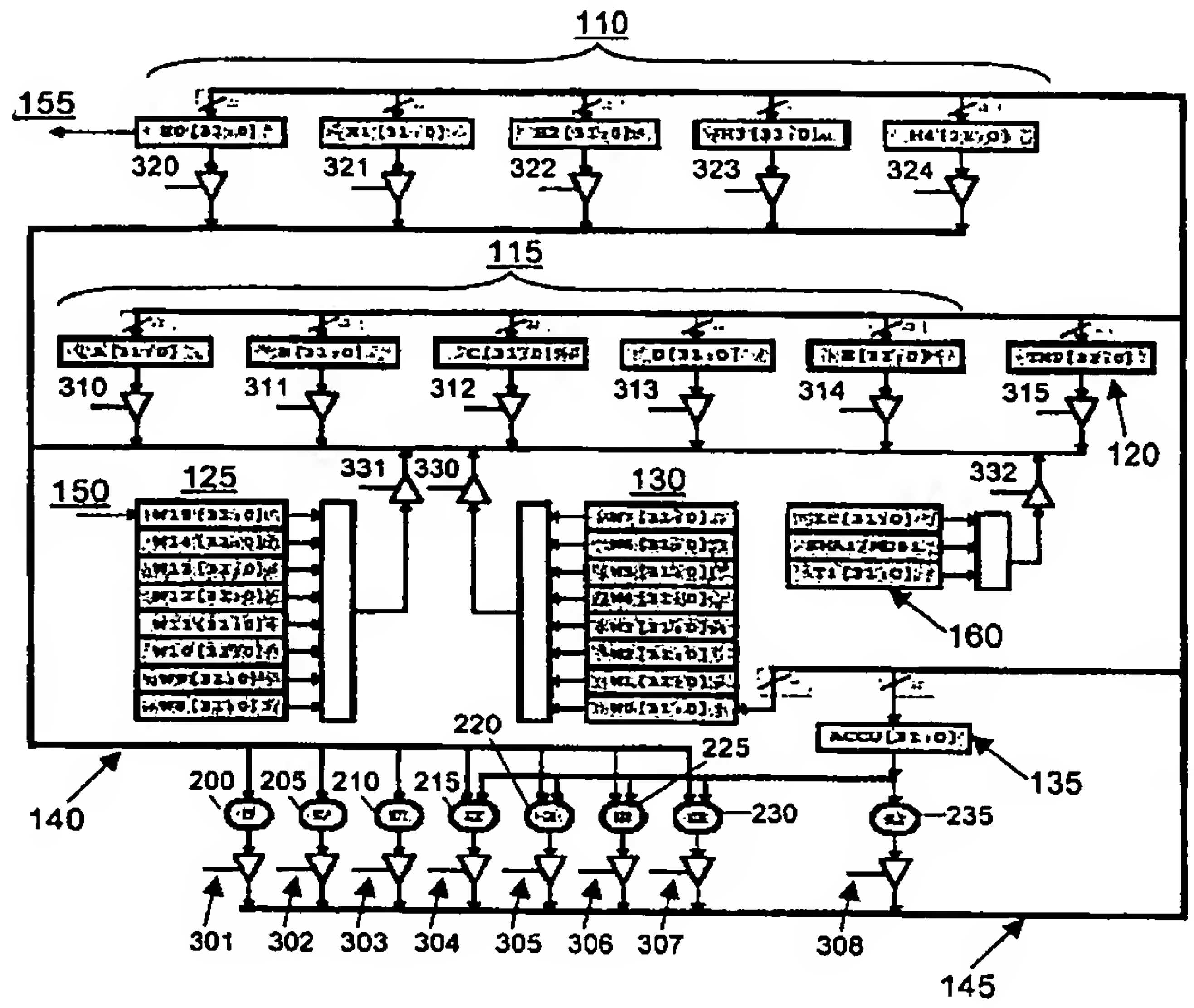
(81) Designated States (*national*): JP, SG, US.

(84) Designated States (*regional*): European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: APPARATUS TO IMPLEMENT DUAL HASH ALGORITHM



(57) Abstract: Apparatus is disclosed which is arranged to accept digital data as an input, and to process said data according to one of either the Secure Hash Algorithm (SHA-1) or Message Digest (MD5) algorithm to produce a fixed length output word. The apparatus includes a plurality of rotational registers for storing data, one of the registers being arranged to receive the input data, and data stores for initialisation of some of said plurality of registers according to whether the SHA-1 or MD5 algorithm is used. The data stores include fixed data relating to SHA-1 and MD5 operation. Also included is a plurality of dedicated combinatorial logic circuits arranged to perform logic operations on data stored in selected ones of said plurality of registers.

WO 2004/042602 A1